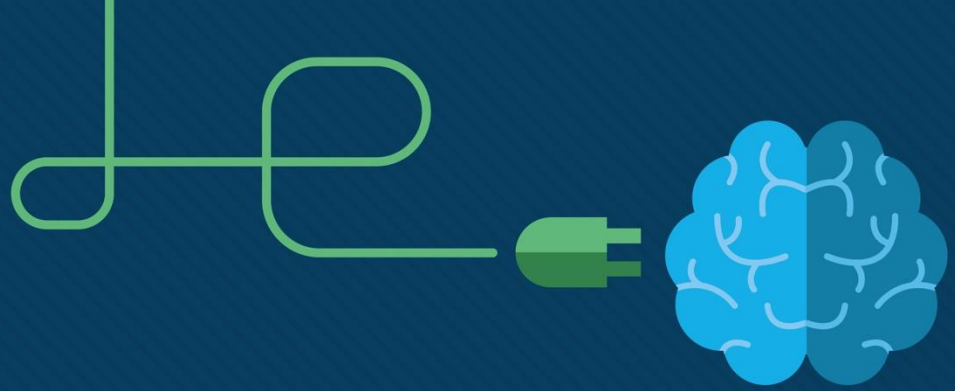


Modül 17: Küçük Bir Ağ Oluşturun

Ağlara Giriş v7.0 (ITN)

Modül Hedefleri

Modü Başlığı: Küçük Bir Ağ Oluşturun

Modül Amacı : Küçük bir ağ için bir yönlendirici, bir anahtar ve uç cihazlar içeren bir ağ tasarımı uygulanması

Konu Başlığı	Amaç
Küçük Bir Ağdaki Cihazlar	Küçük bir ağda kullanılan cihazları tanımlama
Küçük Ağ Uygulamaları ve Protokolleri	Küçük bir ağda kullanılan uygulamaları ve protokolleri tanımlama
Daha Büyük Ağlara Ölçeklendirme	Küçük bir ağın daha büyük ağların temeli olarak nasıl hizmet ettiğinin açıklanması
Bağlantıyı Doğrulama	Bağlantıyı doğrulamak ve göreli ağ performansı oluşturmak için ping ve tracert komutlarının çıktısını kullanma
Host ve IOS Komutları	Bir ağdaki cihazlar hakkında bilgi almak için ana bilgisayar ve IOS komutlarını kullanın
Sorun Giderme Metodojileri	Yaygın sorun giderme metodojilerinin tanımlanması
Sorun Giderme Senaryoları	Ağdaki cihazlar ile ilgili sorunları giderme

17.1 Küçük Bir Ağdaki Cihazlar

Küçük Ağ Topolojileri

- İşletmelerin çoğu küçüktür, iş ağlarının çoğu da küçüktür.
- Küçük bir ağ tasarımı genellikle basittir.
- Küçük ağlar tipik olarak DSL, kablo veya Ethernet bağlantısıyla sağlanan tek bir WAN bağlantısına sahiptir.
- Büyük ağlar, ağ cihazlarının bakımı, güvenliği ve sorunlarını gidermek ve kurumsal verileri korumak için bir BT departmanı gerektirir. Küçük ağlar, yerel bir BT teknisyeni veya sözleşmeli bir profesyonel tarafından yönetilir.

Küçük Ağlar için Cihaz Seçimi

Büyük ağlar gibi, küçük ağlar da kullanıcı gereksinimlerini karşılamak için planlama ve tasarım gerektirir. Planlama, tüm gereksinimlerin, maliyet faktörlerinin ve dağıtım seçeneklerinin gereken şekilde dikkate alınmasını sağlar. İlk tasarım değerlendirmelerinden biri, ağı desteklemek için kullanılacak ara cihazların türüdür.

Ağ cihazlarını seçerken dikkate alınması gereken faktörler şunları içerir:

- Maliyet
- Hız ve bağlantı noktası / arabirim türleri
- Genişletilebilirlik
- İşletim sistemi özellikleri ve hizmetleri

Küçük Ağlar için IP Adresleri

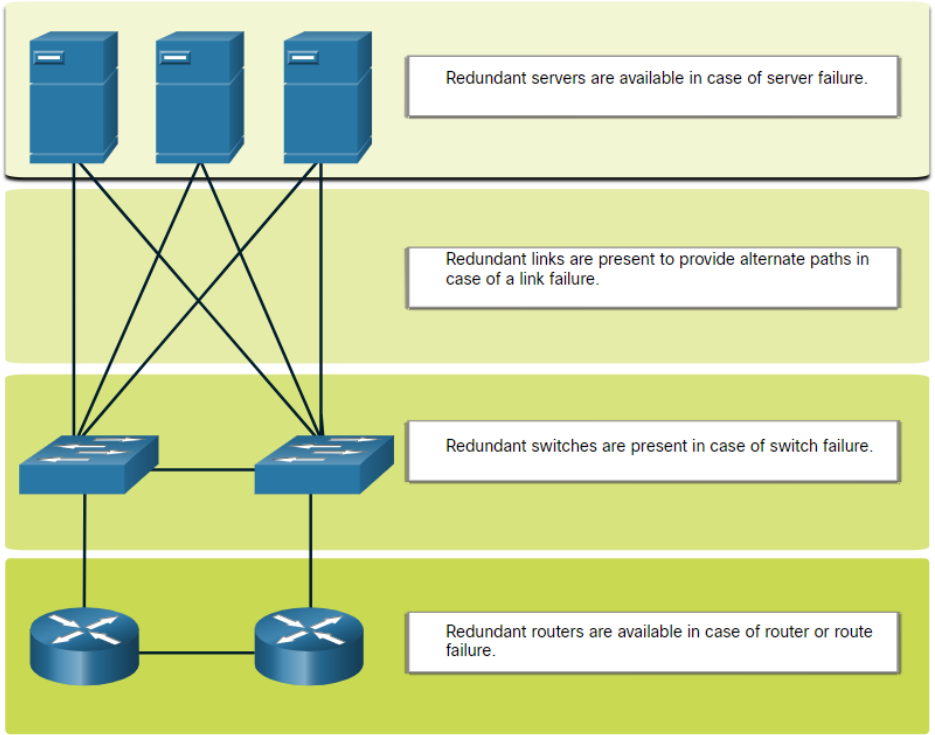
Bir ağ uygularken, bir IP adresleme şeması oluşturun ve kullanın. Bir ağ ağı içindeki tüm ana bilgisayarlar ve cihazlar benzersiz bir adrese sahip olmalıdır. IP adresleme şemasını hesaba katacak cihazlar şunları içerir:

- Son kullanıcı cihazları - Bağlantıların sayısı ve türü (ör. Kablolu, kablosuz, uzaktan erişim)
- Sunucular ve çevre birimleri aygıtları (ör. Yazıcılar ve güvenlik kameraları)
- Anahtarlar ve erişim noktaları dahil aracı cihazlar

Cihaz türüne göre bir IP adresleme şeması planlamanız, belgelemeniz ve sürdürmeniz önerilir. Planlanmış bir IP adresleme şemasının kullanılması, bir cihaz türünü tanımlamayı ve sorunları gidermeyi kolaylaştırır.

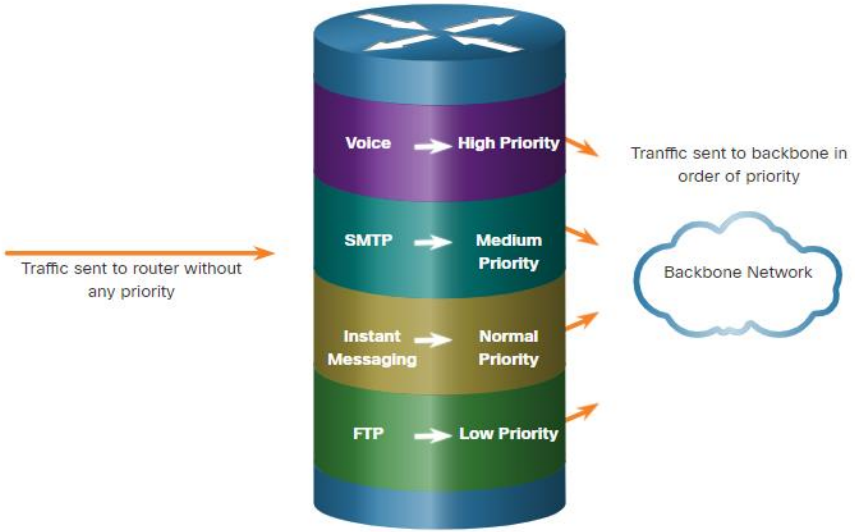
Küçük Ağlarda Yedeklilik

- Yüksek derecede güvenilirlik sağlamak için ağ tasarımında *yedeklilik* gereklidir. Yedeklilik, tek hata noktalarını ortadan kaldırmaya yardımcı olur.
- Yedekleme, yinelenen ekipmanı kurarak gerçekleştirilebilir. Kritik alanlar için yinelenen ağ bağlantıları sağlayarak da gerçekleştirilebilir.



Trafik Yönetimi

- İyi bir ağ tasarımının amacı, çalışanların üretkenliğini artırmak ve ağ kesintilerini en aza indirmektir.
- Küçük bir ağdaki yönlendiriciler ve anahtarlar, ses ve video gibi gerçek zamanlı trafiği, diğer veri trafiğine göre uygun bir şekilde destekleyecek şekilde yapılandırılmalıdır. İyi bir ağ tasarımı hizmet kalitesini (QoS) uygulayacaktır.
- Öncelik kuyruğunun dört kuyruğu vardır. Yüksek öncelikli kuyruk her zaman önce boşaltılır.



17.2 Küçük Ağ Uygulamalar ve Protokoller

Genel Uygulamalar

Kurulumunu yaptıktan sonra, ağınızın çalışması için hala belirli türden uygulamalara ve protokollere ihtiyacı vardır. Ağ, yalnızca üzerinde bulunan uygulamalar kadar kullanışlıdır.

Ağa erişim sağlayan iki tür yazılım programı veya işlemi vardır:

- **Ağ Uygulamaları** : Uygulama katmanı protokollerini uygulayan ve protokol yığınının alt katmanlarıyla doğrudan iletişim kurabilen uygulamalar.
- **Uygulama Katmanı Hizmetleri** : Ağa duyarlı olmayan uygulamalar için, ağ ile arabirim oluşturan ve verileri aktarım için hazırlayan programlar.

Genel Protokoller

Ağ protokolleri, çalışanlar tarafından küçük bir ağda kullanılan uygulamaları ve hizmetleri destekler.

- Ağ yöneticileri genellikle ağ cihazlarına ve sunuculara erişim gerektirir. En yaygın iki uzaktan erişim çözümü Telnet ve Güvenli Kabuk'tur (SSH).
- Hypertext Transfer Protocol (HTTP) ve Hypertext Transfer Protocol Secure (HTTP), web istemcileri ve web sunucuları arasında kullanılır.
- Basit Posta Aktarım Protokolü (SMTP) e-posta göndermek için kullanılır, Postane Protokolü (POP3) veya İnternet Posta Erişim Protokolü (IMAP) istemciler tarafından e-posta almak için kullanılır.
- Dosya Aktarım Protokolü (FTP) ve Güvenlik Dosya Aktarım Protokolü (SFTP), bir istemci ile bir FTP sunucusu arasında dosya indirmek ve yüklemek için kullanılır.
- Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), istemciler tarafından bir DHCP Sunucusundan bir IP yapılandırması almak için kullanılır.
- Alan Adı Hizmeti (DNS), alan adlarını IP adreslerine çözümler.

Not : Bir sunucu birden çok ağ hizmeti sağlayabilir. Örneğin, bir sunucu bir e-posta, FTP ve SSH sunucusu olabilir.

Genel Protokoller (Devam.)

Bu ağ protokolleri, aşağıdakileri tanımlayan bir ağ uzmanının temel araç setini içerir:

- Bir iletişim oturumunun her iki ucundaki işlemler.
- Mesaj türleri.
- Mesajların sözdizimi.
- Bilgi alanlarının anlamı.
- Mesajların nasıl gönderildiği ve beklenen yanıt.
- Bir sonraki alt katmanla etkileşim.

Birçok şirket, mümkün olduğunda bu protokollerin güvenli sürümlerini (örneğin, SSH, SFTP ve HTTPS) kullanma politikası oluşturmuştur.

Ses ve Video Uygulamaları

- Günümüzde işletmeler, müşteriler ve iş ortaklarıyla iletişim kurmak ve çalışanlarının uzaktan çalışmasını sağlamak için giderek daha fazla IP telefonu ve akışlı ortam kullanıyor.
- Ağ yöneticisi, ağa doğru ekipmanın takıldığından ve ağ cihazlarının öncelikli teslimatı sağlayacak şekilde yapılandırıldığından emin olmalıdır.
- Küçük bir ağ yöneticisinin gerçek zamanlı uygulamaları desteklerken göz önünde bulundurması gereken faktörler:
  - **Altyapı -** Gerçek zamanlı uygulamaları destekleme kapasitesi ve yeteneği var mı?
  - **VoIP -** VoIP tipik olarak IP Telefonundan daha ucuzdur, ancak kalite ve özellik pahasına.
  - **IP Telefonu -** Bu, arama kontrolü ve sinyallemeden özel sunucular kullanır.
  - **Gerçek Zamanlı Uygulamalar -** Ağ, gecikme sorunlarını en aza indirmek için Hizmet Kalitesi (QoS) mekanizmalarını desteklemelidir. Gerçek Zamanlı Aktarım Protokolü (RTP) ve Gerçek Zamanlı Aktarım Kontrol Protokolü (RTCP) ve gerçek zamanlı uygulamaları destekleyen iki protokol.

17.3 Daha Büyük Ağlara Ölçeklendirme

Küçük Ağları Büyütme

Büyüme, birçok küçük işletme için doğal bir süreçtir ve ağları buna göre büyümelidir. İdeal olarak, ağ yöneticisinin, ağı şirketin büyümesine paralel olarak büyütme konusunda akıllı kararlar vermek için yeterli ön zamanı vardır.

Bir ağı ölçeklendirmek için birkaç öğe gereklidir:

- **Ağ dokümantasyonu** - Fiziksel ve mantıksal topoloji
- **Cihaz envanteri** - Ağı kullanan veya ağı oluşturan cihazların listesi
- **Bütçe** - Mali yıl ekipman satın alma bütçesi dahil olmak üzere ayrıntılı BT bütçesi
- **Trafik analizi** - Protokoller, uygulamalar ve hizmetler ve bunların ilgili trafik gereksinimleri belgelenmelidir

Bu öğeler, küçük bir ağın ölçeklendirilmesine eşlik eden karar verme sürecini bilgilendirmek için kullanılır.

Protokol Analizi

Ağı geçen trafik türünü ve mevcut trafik akışını anlamak önemlidir. Bu amaçla kullanılabilecek birkaç ağ yönetim aracı vardır.

Trafik akış modellerini belirlemek için aşağıdakileri yapmak önemlidir:

- Farklı trafik türlerinin iyi bir temsilini elde etmek için yoğun kullanım zamanlarında trafiği yakalayın.
- Yakalama işlemini farklı ağ segmentlerinde ve cihazlarda gerçekleştirin çünkü trafik belirli bir segment için yerel olacaktır.
- Protokol analizcisi tarafından toplanan bilgiler, trafiğin kaynağı ve hedefi ile gönderilen trafiğin türüne göre değerlendirilir.
- Bu analiz, trafiğin daha verimli bir şekilde nasıl yönetileceğine dair kararlar almak için kullanılabilir.

Çalışan Ağ Kullanımı

Çoğu işletim sistemi, bu tür ağ kullanım bilgilerini görüntülemek için yerleşik araçlar sağlar. Bu araçlar, aşağıdaki gibi bilgilerin bir "anlık görüntüsünü" yakalamak için kullanılabilir:

- İşletim Sistemi ve İşletim Sistemi Sürümü
- CPU kullanımı
- RAM kullanımı
- Sürücü kullanımı
- Ağ dışı uygulamalar
- Ağ uygulamaları

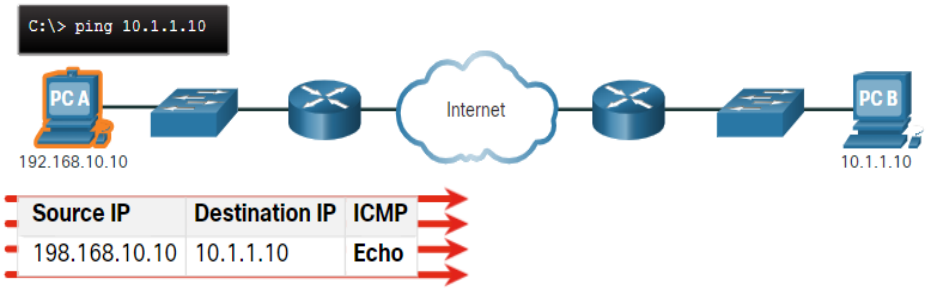
Küçük bir ağdaki çalışanlar için belirli bir süre anlık görüntülerin belgelenmesi, gelişen protokol gereksinimlerini ve ilgili trafik akışlarını belirlemek için çok yararlıdır.

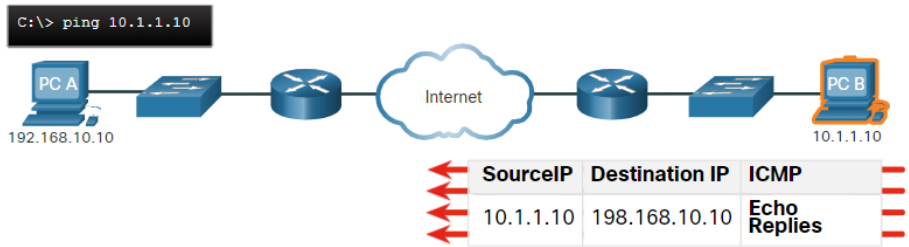
17.4 Bağlantıyı Doğrulama

Ping ile Bağlantıyı Doğrulama

Ağınız ister küçük ve yeni olsun, ister mevcut bir ağı ölçeklendiriyor olun, bileşenlerinizin birbirine ve internete doğru şekilde bağlandığını her zaman doğrulayabilmek isteyeceksiniz.

- Çoğu işletim sisteminde bulunan ping komutu, bir kaynak ve hedef IP adresi arasındaki Katman 3 bağlantısını hızlı bir şekilde test etmenin en etkili yoludur.
- Ping komutu İnternet Kontrol Mesajı Protokolü (ICMP) yankısı (ICMP Tip 8) ve yankı yanıtı (ICMP Tip 0) mesajlarını kullanır.





Ping ile Bağlantıyı Doğrulayın (Devam)

Windows 10 ana bilgisayarında, ping komutu art arda dört ICMP yankı iletisi gönderir ve hedeften art arda dört ICMP yankı yanıtı bekler. IOS ping, beş ICMP yankı mesajı gönderir ve alınan her ICMP yankı yanıtı için bir gösterge görüntüler.

IOS Ping Göstergeleri aşağıdaki gibidir:

Element	Açıklama
!	• Ünlem işareti, bir yankı yanıt mesajının başarıyla alındığını gösterir. • Kaynak ve hedef arasındaki Katman 3 bağlantısını doğrular.
.	• Bir süre, bir yankı yanıtı mesajı bekleyerek sürenin dolduğu anlamına gelir. • Bu, yol üzerinde bir yerde bağlantı sorunu olduğunu gösterir.
U	• Büyük ”**U”** harfi , ICMP Tip 3 "hedef ulaşılamaz" hata mesajıyla yanıtlanan yol üzerindeki bir yönlendiriciyi belirtir. • Olası nedenler arasında yönlendiricinin hedef ağın yönünü bilmemesi veya hedef ağda ana bilgisayarı bulamaması yer alır.

Not: Diğer olası ping yanıtları arasında Q, M,? Veya & bulunur. Ancak bunların anlamı bu modül için kapsam dışındadır.

Genişletilmiş Ping

Cisco IOS, ping komutunun "genişletilmiş" bir modunu sunar .

Genişletilmiş ping, ayrıcalıklı EXEC modunda hedef IP adresi olmadan ping yazılarak girilir . Daha sonra genişletilmiş pingi özelleştirmeniz için size birkaç komut verilecektir .

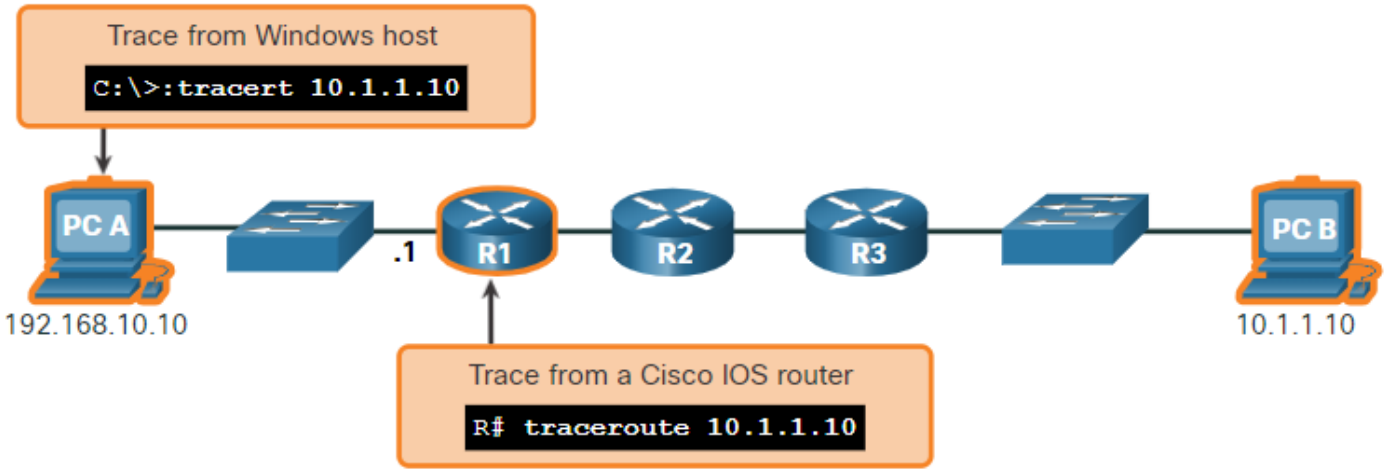
Not: Enter tuşuna basılması , belirtilen varsayılan değerleri kabul eder. Ping ipv6 IPv6 için kullanılan komut pingleri uzatıldı.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

Traceroute ile Bağlantıyı Doğrulama

Ping komutu, Katman 3 bağlantı sorunu olup olmadığını hızlı bir şekilde belirlemek için kullanışlıdır. Ancak, sorunun yol boyunca nerede olduğunu belirlemez.

- İzleme yolu, bir ağdaki Katman 3 sorunlu alanların bulunmasına yardımcı olabilir. Bir izleme, bir paket ağ üzerinden yönlendirilirken bir atlama listesi döndürür.
- Trace komutunun sözdizimi işletim sistemleri arasında değişiklik gösterir.



Traceroute ile Bağlantıyı Doğrulama (Devam)

Aşağıda, bir Windows 10 ana bilgisayarında **tracert** komutunun örnek bir çıktısı verilmiştir .

Not: Windows'ta bir izlemeyi kesmek için Ctrl-C tuşlarını kullanın .

Tek başarılı yanıt, R1'deki ağ geçidinden geldi. Bir sonraki atlama için izleme istekleri yıldız işaretiyle (*) gösterildiği gibi zaman aşımına uğradı, bu, sonraki atlama yönlendiricisinin yanıt vermediği veya ağ yolunda bir arıza olduğu anlamına gelir. Bu örnekte, R1 ve R2 arasında bir sorun var gibi görünüyor.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

Traceroute ile Bağlantıyı Doğrulama (Devam)

Aşağıdakiler, R1'den traceroute komutunun örnek çıktılarıdır:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3  *  *  *
  4  *  *  *
  5  *
```

Solda, ”trace” PC B'ye başarıyla ulaşabileceğini doğruladı.
Sağda, 10.1.1.10 ana bilgisayarı kullanılamıyordu ve çıktı, yanıtların zaman aşımına uğradığı yıldız işaretlerini gösteriyor. Zaman aşımları, olası bir ağ sorununu gösterir.
Cisco IOS’ta **traceroute** kesmek için **Ctrl-Shift-6 tuşlarını** kullanın .

Not : Windows uygulaması traceroute (tracert), ICMP Yankı İstekleri gönderir. Cisco IOS ve Linux, geçersiz bir bağlantı noktası numarasıyla UDP kullanır. Son hedef, bir ICMP bağlantı noktasına erişilemez mesajı döndürecektir.

Genişletilmiş Traceroute

Genişletilmiş ping komutu gibi, genişletilmiş **traceroute** komutu da vardır. Yöneticinin komut işlemiyle ilgili parametreleri ayarlamasına izin verir.

Windows **tracert** komutu, komut satırındaki seçenekler aracılığıyla birkaç parametrenin girilmesine izin verir. Ancak, genişletilmiş traceroute IOS komutu gibi yönlendirilmez. Aşağıdaki çıktı, Windows **tracert** komutu için mevcut seçenekleri görüntüler :

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
C:\Users\PC-A>
```

Genişletilmiş Traceroute (Devam)

Cisco IOS genişletilmiş **traceroute** seçeneği, kullanıcının komut işlemiyle ilgili parametreleri ayarlayarak özel bir izleme türü oluşturmasını sağlar.

Genişletilmiş traceroute, hedef IP adresi olmadan **traceroute** yazarak ayrıcalıklı EXEC modunda girilir . IOS, tüm farklı parametrelerin ayarlanmasıyla ilgili bir dizi bilgi istemi sunarak komut seçeneklerinde size rehberlik edecektir.

Not : **Enter** tuşuna basılması , belirtilen varsayılan değerleri kabul eder.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

Ağ Tabanı

- Ağ performansını izlemek ve sorun gidermek için en etkili araçlardan biri, bir ağ temeli oluşturmaktır.
- Bir temel başlatmanın bir yöntemi, yürütülen bir ping, izleme veya diğer ilgili komutlardan alınan sonuçları kopyalayıp bir metin dosyasına yapıştırmaktır. Bu metin dosyalarına tarih eklenebilir ve daha sonra geri çağırma ve karşılaştırma için bir arşive kaydedilebilir.
- Dikkate alınacak öğeler arasında hata mesajları ve ana bilgisayardan ana bilgisayara yanıt süreleri vardır.
- Kurumsal ağlar bu kursta tanımlayabileceğimizden daha kapsamlı temellere sahiptir . Temel bilgileri depolamak ve işlemek için profesyonel düzeyde yazılım araçları mevcuttur.

Lab –Ping ve Traceroute ile Ağ Gecikme Testi

Bu laboratuvarda , aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Ping Göndererek Ağ Gecikmesisini belgeleme
- Bölüm 2: Ağ Gecikmesini Belgelemek İçin Traceroute Kullanma

17.5 Host ve IOS Komutları

Windows Host üzerinde IP Konfigürasyonu

Windows 10'da, dört önemli ayarı hızlı bir şekilde görüntülemek için Ağ ve Paylaşım Merkezi'nden IP adresi ayrıntılarına erişebilirsiniz : adres, maske, yönlendirici ve DNS. Veya **ipconfig** komutunu bir Windows bilgisayarın komut satırından da verebilirsiniz .

- MAC adresini ve cihazın L3 adreslemesine ilişkin bir dizi ayrıntıyı görüntülemek için **ipconfig / all** komutunu kullanın.
- Bir ana bilgisayar bir DHCP istemcisi olarak yapılandırılmışsa, IP adresi yapılandırması **ipconfig / release** ve **ipconfig / renew** komutları kullanılarak yenilenebilir .
- Windows PC'lerdeki DNS İstemci hizmeti, önceden çözümlenmiş adları bellekte depolayarak DNS adı çözümlemesinin performansını da optimize eder. **İpconfig / displaydns** tüm Windows bilgisayar sisteminde önbelleğe DNS girdilerinin görüntüler komuta.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Linux Host üzerinde IP Konfigürasyonu

- Bir Linux makinesinde GUI kullanılarak IP ayarlarının doğrulanması, Linux dağıtımına ve masaüstü arayüzüne bağlı olarak farklılık gösterecektir.
- Komut satırında, şu anda etkin olan arabirimlerin durumunu ve IP yapılandırmalarını görüntülemek için **ifconfig** komutunu kullanın.
- Linux **ip adresi** komutu, adresleri ve özelliklerini görüntülemek için kullanılır. IP adreslerini eklemek veya silmek için de kullanılabilir.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Not: Görüntülenen çıktı, Linux dağıtımına bağlı olarak değişebilir.

MacOS Host üzerinde IP Konfigürasyonu

- Bir Mac ana bilgisayarının GUI'sinde , IP adresleme bilgilerini almak için **Ağ Tercihleri> Gelişmiş'i** açın .
- **İfconfig** komutu komut satırında arayüzü IP yapılandırmasını doğrulamak için kullanılabilir.
- Ana bilgisayar IP ayarlarını doğrulamak için diğer yararlı macOS komutları arasında **networksetup -listallnetworkservices** ve **networksetup -getinfo** <network service> .

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

“arp” Komutu

Arp komutu Windows, Linux veya Mac komut isteminden çalıştırılır. Komut, şu anda ana bilgisayarın ARP önbelleğinde bulunan tüm cihazları listeler.

- **Arp -a** komut bilinen IP adresi ve MAC adresi bağlayıcı. ARP önbelleği yalnızca son erişilen cihazlardan gelen bilgileri görüntüler.
- ARP önbelleğinin doldurulduğundan emin olmak için, bir aygıta ARP tablosunda bir giriş olacak şekilde **ping** atın.
- Önbellek , ağ yöneticisinin önbelleği güncellenmiş bilgilerle yeniden doldurmak **istemesi** durumunda **netsh arabirimi ip delete arpcache** komutu kullanılarak temizlenebilir .

Not : netsh interface ip delete arpcache komutunu kullanabilmek için ana bilgisayarda yönetici erişimine ihtiyacınız olabilir .

Yaygın "show" Komutları

Komut	Açıklama
show running-config	Mevcut yapılandırmayı ve ayarları doğrular
show interfaces	Arayüz durumunu doğrular ve tüm hata mesajlarını görüntüler
show ip interface	Bir arayüzün Katman 3 bilgilerini doğrular
show arp	Yerel Ethernet LAN'larındaki bilinen ana bilgisayarların listesini doğrular
show ip route	Katman 3 yönlendirme bilgilerini doğrular
show protocols	Hangi protokollerin çalıştığını doğrular
show version	Cihazın hafızasını, arayüzlerini ve lisanslarını doğrular

“show cdp neighbors” Komutu

CDP, her bir CDP komşu cihazı hakkında aşağıdaki bilgileri sağlar:

- **Cihaz tanımlayıcıları** - Bir anahtarın, yönlendiricinin veya başka bir cihazın yapılandırılmış ana bilgisayar adı
- **Adres listesi** - Desteklenen her protokol için bir ağ katmanı adresine kadar
- **Port tanımlayıcısı** - FastEthernet 0/0 gibi bir ASCII karakter dizesi biçimindeki yerel ve uzak bağlantı noktasının adı
- **Yetenekler listesi** - Belirli bir cihazın Katman 2 anahtarı mı yoksa Katman 3 anahtarı mı olduğu
- **Platform** - Cihazın donanım platformu.

show cdp neighbors detail komutu bir komşu cihazın IP adresini ortaya koymaktadır.

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

“show ip interface brief” Komutu

En sık kullanılan komutlardan biri **show ip interface brief** komutudur. Bu komut **show ip interface** komutundan daha kısaltılmış bir çıktı sağlar . Bir yönlendiricideki tüm ağ arayüzleri için önemli bilgilerin bir özetini sağlar.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.254.250 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
```

Video –”show version” Komutu

Bu video, yönlendirici hakkındaki bilgileri görüntülemek için show version komutunu kullanmayı gösterecektir.

Packet Tracer – “Interpret show” Komutu Çıktısı

Bu etkinlik, yönlendirici ”show” komutlarının kullanımını güçlendirmek için tasarlanmıştır . Yapılandırmanız gerekmez, bunun yerine birkaç show komutunun çıktısını analiz etmeniz gerekir.

17.6 Sorun Giderme Metedolojileri

Temel Sorun Giderme Yaklaşımları

Adım	Açıklama
Adım 1. Sorunu Belirleyin	• Bu, sorun giderme sürecinin ilk adımıdır. • Bu adımda araçlar kullanılabilse de, kullanıcıyla konuşmak genellikle çok faydalıdır.
Adım 2. Olası Nedenler Teorisi Oluşturun	•Sorun belirlendikten sonra, olası nedenlerle ilgili bir teori oluşturmaya çalışın. •Bu adım genellikle soruna birkaç olası nedenden fazlasını verir.
Adım 3. Nedeni Belirlemek için Teoriyi Test Edin	•Olası nedenlere bağlı olarak, sorunun nedeninin hangisi olduğunu belirlemek için teorilerinizi test edin. •Bir teknisyen, test etmek ve sorunu çözüp çözmediğini görmek için hızlı bir düzeltme uygulayabilir. •Hızlı bir düzeltme sorunu çözmezse, kesin nedenini belirlemek için sorunu daha fazla araştırmanız gerekebilir.
Adım 4. Bir Eylem Planı Oluşturun ve Çözümü Uygulayın	Sorunun kesin nedenini belirledikten sonra, sorunu çözmek ve çözümü uygulamak için bir eylem planı oluşturun.
Adım 5. Çözümü Doğrulayın ve Önleyici Tedbirler Uygulayın	•Sorunu düzelttikten sonra tam işlevselliği doğrulayın. •Mümkünse, önleyici tedbirler uygulayın.
Adım 6. Bulguları, Eylemleri ve Sonuçları Belgeleyin	•Sorun giderme sürecinin son adımında bulgularınızı, eylemlerinizi ve sonuçlarınızı belgeleyin. •Bu ileride başvurmak için çok önemlidir.

Çözüm veya Yükseltme?

- Bazı durumlarda sorunu hemen çözmek mümkün olmayabilir. Bir yönetici kararı, belirli bir uzmanlık veya sorun giderme teknisyeninin erişemeyeceği ağ erişim düzeyi gerektirdiğinde bir sorun yükseltilmelidir.
- Bir şirket politikası, bir teknisyenin bir sorunu ne zaman ve nasıl yükseltmesi gerektiğini açıkça belirtmelidir.

“debug” Komutu

- IOS **debug** komutu, yöneticinin analiz için işletim sistemi sürecini, protokolünü, mekanizmasını ve olay mesajlarını gerçek zamanlı olarak görüntülemesini sağlar.
- Tüm **debug** komutları ayrıcalıklı EXEC modunda girilir. Cisco IOS, **debug** çıktısını yalnızca ilgili özelliği veya alt özelliği içerecek şekilde daraltmaya izin verir . **Debug** komutlarını yalnızca belirli sorunları gidermek için kullanın .
  - Tüm hata ayıklama komut seçeneklerinin kısa bir açıklamasını listelemek için “**debug ?”** komutu kullanılır .
  - Belirli bir hata ayıklama özelliğini kapatmak için **debug** komutunun önüne ” **no** ” ekleyin
  - Alternatif olarak, ayrıcalıklı EXEC modunda komutun **debug** biçimini girebilirsiniz .
  - Aynı anda tüm aktif ayıklama komutları kapatmak için, **undebug all** komutu.
- Bazı **debug** komutlarını kullanırken dikkatli olun , çünkü bunlar önemli miktarda çıktı üretebilir ve sistem kaynaklarının büyük bir bölümünü kullanabilir. Yönlendirici, **debug** mesajlarını görüntüleyerek o kadar meşgul olabilir ki, ağ işlevlerini gerçekleştirmek için yeterli işlem gücüne sahip olmayabilir, hatta hata ayıklamayı kapatmak için komutları bile dinleyebilir.

“terminal monitor” Komutu

- **debug** ve belirli diğer IOS mesaj çıktısı uzak bağlantılarda otomatik olarak görüntülenmez. Bunun nedeni, günlük mesajlarının vty satırlarında görüntülenmesinin engellenmesidir.
- Günlük mesajlarını bir terminalde (sanal konsol) görüntülemek için, **terminal monitor** privileged EXEC komutunu kullanın. Bir terminalde mesajların günlüğe kaydedilmesini durdurmak için ”no **terminal monitor** privileged EXEC” komutunu kullanın.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
 Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

```
R1#  terminal monitor
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

17.7 Sorun Giderme Senaryoları

Çift Taraflı İşlem ve Uyumsuzluk Sorunları

- Birbirine bağlanan Ethernet arayüzleri, en iyi iletişim performansı için ve bağlantıda verimsizlik ve gecikmeyi önlemek için aynı çift yönlü modda çalışmalıdır.
- Ethernet otomatik anlaşma özelliği, yapılandırmayı kolaylaştırır, sorunları en aza indirir ve birbirine bağlanan iki Ethernet bağlantısı arasındaki bağlantı performansını en üst düzeye çıkarır. Bağlı cihazlar önce desteklenen yeteneklerini duyurur ve ardından her iki tarafın da desteklediği en yüksek performans modunu seçer.
- Bağlı iki aygıttan biri tam çift yönlü, diğeri yarı çift yönlü çalışıyorsa, çift yönlü uyumsuzluk oluşur. Veri iletişimi, çift yönlü uyumsuzluğa sahip bir bağlantı yoluyla gerçekleşecek olsa da, bağlantı performansı çok zayıf olacaktır.
- Çift yönlü uyuşmazlıklar genellikle yanlış yapılandırılmış bir arabirimden veya nadir durumlarda başarısız bir otomatik anlaşmadan kaynaklanır. Cihazlar arasındaki iletişim devam ettiği için çift yönlü uyumsuzlukları gidermek zor olabilir.

IOS Cihazlarında IP Adresleme Sorunları

- Yanlış IPv4 atamasının iki yaygın nedeni, manuel atama hataları veya DHCP ile ilgili sorunlardır.
- Ağ yöneticilerinin genellikle sunucular ve yönlendiriciler gibi cihazlara manuel olarak IP adresi ataması gerekir. Atama sırasında bir hata yapılırsa, büyük olasılıkla cihazla iletişim sorunları yaşanır.
- Bir IOS aygıtında, ağ arabirimlerine hangi IPv4 adreslerinin atandığını doğrulamak için **show ip interface** veya **show ip interface brief** komutlarını kullanın. Örneğin, gösterildiği gibi show ip interface brief komutunun verilmesi, R1'deki arayüz durumunu doğrular.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

Son Kullanıcı Cihazlarında IP Adresleme Sorunları

- Windows tabanlı makinelerde, cihaz bir DHCP sunucusuyla bağlantı kuramadığında, Windows otomatik olarak 169.254.0.0/16 aralığına ait bir adres atayacaktır. Bu özelliğe Otomatik Özel IP Adresleme (APIPA) denir.
- APIPA adresine sahip bir bilgisayar, ağdaki diğer cihazlarla iletişim kuramaz çünkü bu cihazlar büyük olasılıkla 169.254.0.0/16 ağına ait olmayacaktır.
  - **Not** : Linux ve OS X gibi diğer işletim sistemleri APIPA kullanmaz.
- Aygıt DHCP sunucusuyla iletişim kuramıyorsa, sunucu belirli ağ için bir IPv4 adresi atayamaz ve aygıt iletişim kuramaz.
- Windows tabanlı bir bilgisayara atanan IP adreslerini doğrulamak için **ipconfig** komutunu kullanın.

Varsayılan Ağ Geçidi Sorunları

- Bir son cihaz için varsayılan ağ geçidi, trafiği diğer ağlara iletebilen son cihazla aynı ağa ait olan en yakın ağ cihazıdır. Bir aygıt yanlış veya var olmayan bir varsayılan ağ geçidi adresine sahipse, uzak ağlardaki aygıtlarla iletişim kuramayacaktır.
- IPv4 adresleme sorunlarına benzer şekilde, varsayılan ağ geçidi sorunları, yanlış yapılandırma (manuel atama durumunda) veya DHCP sorunları (otomatik atama kullanımdaysa) ile ilgili olabilir.
- Windows tabanlı bilgisayarlarda varsayılan ağ geçidini doğrulamak için **ipconfig** komutunu kullanın.
- Bir yönlendiricide, yönlendirme tablosunu listelemek ve varsayılan yol olarak bilinen varsayılan ağ geçidinin ayarlandığını doğrulamak için **show ip route** komutunu kullanın. Bu yol, paketin hedef adresi yönlendirme tablosundaki diğer yollarla eşleşmediğinde kullanılır.

DNS Sorunları Giderme

- Kullanıcıların yanlışlıkla bir internet bağlantısının çalışmasını DNS'nin kullanılabilirliğiyle ilişkilendirmesi yaygındır.
- DNS sunucusu adresleri manuel veya otomatik olarak DHCP aracılığıyla atanabilir.
- Şirketlerin ve kuruluşların kendi DNS sunucularını yönetmeleri yaygın olsa da, herhangi bir erişilebilir DNS sunucusu adları çözümlemek için kullanılabilir.
- Cisco, kimlik avı ve bazı kötü amaçlı yazılım sitelerini filtreleyerek güvenli DNS hizmeti sağlayan OpenDNS sunar. OpenDNS adresleri 208.67.222.222 ve 208.67.220.220'dir. Web içeriği filtreleme ve güvenlik gibi gelişmiş özellikler aileler ve işletmeler tarafından kullanılabilir.
- Windows bilgisayarı tarafından hangi DNS sunucusunun kullanıldığını doğrulamak için **ipconfig / all** komutunu gösterildiği gibi kullanın.
- **Nslookup** komutu PC'ler için başka bir faydalı bir DNS sorun giderme aracıdır. İle **nslookup** bir kullanıcı manuel olarak DNS sorgularını yerleştirmek ve DNS tepkisini analiz edebilirsiniz.

Lab – Bağlantı Sorunlarını Giderme

Bu laboratuvarda , aşağıdaki hedefleri tamamlayacaksınız:

- Sorunu Tanımlayın
- Ağ Değişikliklerini Uygulayın
- Tam İşlevselliği Doğrulayın
- Belge Bulguları ve Yapılandırma Değişiklikleri

Packet Tracer – Bağlantı Sorunlarını Giderme

Bu Packet Tracer etkinliğinin amacı, mümkünse bağlantı sorunlarını gidermek ve çözmektir. Aksi takdirde, sorunlar açıkça belgelendirilmeli ve böylece yükseltilebilir olmalıdır.

17.8 Alıştırmalar ve Sınav

Lab – Bir Küçük İşletme Ağı Tasarlayın ve Oluşturun

Bu laboratuvarda bir ağ tasarlayacak ve inşa edeceksiniz. Doğrudan bağlı segmentlerden oluşan küçük bir ağın nasıl oluşturulduğunu, yapılandırıldığını ve doğrulandığını açıklayacaksınız.

Packet Tracer – Beceri Entegrasyon Zorluğu

Bu Packet Tracer etkinliğinde, bu kurs boyunca edindiğiniz tüm becerileri kullanacaksınız.

Senaryo:

Yönlendirici Merkezi, ISP kümesi ve Web sunucusu tamamen yapılandırılmıştır. 192.168.0.0/24 ağını kullanarak 4 alt ağı barındıracak yeni bir IPv4 adresleme şeması oluşturmalısınız. BT departmanı 25 ana bilgisayara ihtiyaç duyar. Satış departmanının 50 ana bilgisayara ihtiyacı var. Personelin geri kalanı için alt ağ 100 ana bilgisayar gerektirir. Gelecekte 25 ana bilgisayarı barındıracak bir Konuk alt ağı eklenecektir. Ayrıca R1'de temel güvenlik ayarlarını ve arayüz yapılandırmalarını da bitirmelisiniz. Ardından, SVI arayüzünü ve S1, S2 ve S3 anahtarlarındaki temel güvenlik ayarlarını yapılandıracaksınız

Packet Tracer – “Sorun Giderme”

Bu Packet Tracer etkinliğinde, mevcut bir LAN'daki bir dizi sorunu giderecek ve çözeceksiniz.

Bu modülde ne öğrendim ?

- Küçük bir ağ için ağ cihazlarını seçerken göz önünde bulundurulması gereken faktörler maliyet, hız ve bağlantı noktası / arayüz türleri, genişletilebilirlik ve işletim sistemi özellikleri ve hizmetleridir.
- Bir ağ uygularken, bir IP adresleme şeması oluşturun ve bunu uç cihazlarda, sunucularda ve çevre birimlerinde ve ara cihazlarda kullanın.
- Yedekleme, yinelenen ekipman kurarak gerçekleştirilebilir, ancak kritik alanlar için yinelenen ağ bağlantıları sağlayarak da gerçekleştirilebilir.
- Küçük bir ağdaki yönlendiriciler ve anahtarlar, ses ve video gibi gerçek zamanlı trafiği, diğer veri trafiğine göre uygun bir şekilde destekleyecek şekilde yapılandırılmalıdır.
- Ağa erişim sağlayan iki tür yazılım programı veya işlemi vardır: ağ uygulamaları ve uygulama katmanı hizmetleri.
- Bir ağı ölçeklendirmek için birkaç öğe gereklidir: ağ dokümantasyonu, cihaz envanteri, bütçe ve trafik analizi.
- Ping komutu, bir kaynak ve hedef IP adresi arasındaki Katman 3 bağlantısını hızlı bir şekilde test etmenin en etkili yoludur.
- Cisco IOS, kullanıcının komut işlemiyle ilgili parametreleri ayarlayarak özel ping türleri oluşturmasına izin veren "genişletilmiş" bir ping komutu modu sunar.

Bu modülde ne öğrendim ?

- Bir izleme, bir paket ağ üzerinden yönlendirilirken bir atlama listesi döndürür.
- Ayrıca genişletilmiş bir iz yolu komutu da vardır. Yöneticinin komut işlemiyle ilgili parametreleri ayarlamasına izin verir.
- Ağ yöneticileri, ipconfig komutunu vererek bir Windows ana bilgisayarındaki IP adresleme bilgilerini (adres, maske, yönlendirici ve DNS) görüntüler. Diğer gerekli komutlar **ipconfig / all , ipconfig / release ve ipconfig / renew ve ipconfig / displaydns**'dir .
- Bir Linux makinesinde GUI kullanarak IP ayarlarının doğrulanması, Linux dağıtımına (dağıtım) ve masaüstü arayüzüne bağlı olarak farklılık gösterecektir. Gerekli komutlar ifconfig ve ip adresidir.
- Bir Mac host GUI'sinde, IP adresleme bilgilerini almak için Ağ Tercihleri> Gelişmiş'i açın. Mac için diğer IP adresleme komutları ifconfig ve networksetup -listallnetworkservices ve networksetup -getinfo <ağ hizmeti> dir.
- **Arp** komutu Windows, Linux veya Mac komut isteminden çalıştırılır. Komut, her cihaz için IPv4 adresini, fiziksel adresi ve adresleme türünü (statik / dinamik) içeren ana bilgisayarın ARP önbelleğinde bulunan tüm cihazları listeler.
- **Arp -a** komut bilinen IP adresi ve MAC adresi bağlayıcı.

Bu modülde ne öğrendim ?

- Ortak “show komutları **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, ve **show version ‘** dır. **show cdp neighbor** komutu her CDP cihaz hakkında aşağıdaki bilgileri sağlar : Tanımlayıcılar , addres listesi, port tanımlayıcıları, kabiliyet listesi ve platform
- **“show cdp neighbors detail”** komutu CDP komşularından birinin bir IP yapılandırması hata varsa komut belirlemek yardımcı olacaktır.
- **“show ip interface brief”** komutu çıktısı **,** yönlendiri üzerindeki tüm bağlantı arabirimlerini , her bir arabirime atanan IP adreslerini ve arabirimlerin operasyonel durumlarını gösterir.
- Sorun gidermeye yönelik altı temel adım : Adım 1. Sorunu belirleme Adım 2. Muhtemel nedenlerle ilgili bir teori oluşturun. Adım 3. Nedeni belirlemek için teoriyi test edin. Adım 4. Bir eylem planı oluşturun ve çözümü uygulayın. Adım 5. Çözümü doğrulayın ve önleyici tedbirleri uygulayın. Adım 6. Bulguları, eylemleri ve sonuçları belgeleyin.
- Bir yöneticinin kararını, belirli bir uzmanlığı veya sorun giderme teknisyeninin erişemeyeceği ağ erişim düzeyini gerektirdiğinde bir sorun yükseltilmelidir.
- İşletim sistemi süreçleri, protokolleri, mekanizmaları ve olayları, durumlarını bildirmek için mesajlar üretir. IOS hata ayıklama komutu, yöneticinin bu mesajları analiz için gerçek zamanlı olarak görüntülemesini sağlar.
- Günlük mesajlarını bir terminalde (sanal konsol) görüntülemek için, terminal monitor privileged EXEC komutunu kullanın.


CISCO